Federal Bridge CA Certificate Policy
Change Proposal

Change Serial Number: 2002-01

Title: Clarify FBCA requirements to facilitate policy mapping

Date: 29 May 2002

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 11 February 2002

Change Advocates Contact Information:

Name: Tim Polk
Organization: NIST
Telephone number: (301) 975-3348
E-mail address: tim.polk@nist.gov

Name: John Cornell
Organization: GSA
Telephone number: (202) 501-1598
E-mail address: john.cornell@gsa.gov

Organization requesting change: CPWG

Change summary: The FBCA CPWG recommends the following changes as a result of the DoD and NASA Policy Mapping exercise. Seventeen items are included in this change proposal. Details for each item follow.

Background:

The FBCA CPWG met on 28 March, 9 May, and 10 May 2002 to review the detailed mapping comparison of the FBCA CP (Medium Assurance Level) and the DoD and NASA CPs. The DoD CP was compared based on the Class 3 Assurance Level certificate policy. (The NASA CP is a single level policy.)

The following conventions are used to depict specific changes: language deleted appears as ~~strikethrough~~; language inserted appears as <u>underlined.</u>

Specific Changes:

Item 1, Section 2.7.5

2.7.5 Actions taken as a result of deficiency

The Federal PKI Policy Authority may determine that the FBCA or Agency CA is not complying with its obligations set forth in this CP or the respective MOA. When such a determination is made, the Federal PKI Policy Authority may suspend operation of the FBCA, or may direct the FBCA Operational Authority to cease interoperating with the affected Agency Principal CA (e.g., by revoking the certificate that the FBCA had issued to the Agency Principal CA), or may direct that other corrective actions be taken which allow interoperation to continue. When the compliance auditor finds a discrepancy between how the FBCA or Agency CA is designed or is being operated or maintained, and the requirements of this CP, the Agency CP, ~~or~~ the MOA, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Agency of the discrepancy. If the discrepancy is judged by the Agency to be severe in nature (that is, it is determined to be a "material discrepancy" relative to the applicable requirements), the Agency shall notify the Federal PKI Policy Authority promptly;
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the MOA, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Federal PKI Policy Authority may decide to halt temporarily operation of the FBCA, to revoke a certificate issued by the FBCA, or take other actions it deems appropriate. The Federal PKI Policy Authority will develop procedures for making and implementing such determinations.

Item 2, Section 3.1.4

3.1.4 Uniqueness of names

Name uniqueness across the FPKI must be enforced. The FBCA, Agency CAs and RAs shall enforce name uniqueness within the X.500 name space which they have been authorized. When ~~other~~ name forms other than a DN (e.g., an electronic mail address or DNS name) are used, they too must be allocated such that name uniqueness across the FPKI is ensured.

The FBCA ~~and Agency CAs~~ shall document in ~~their respective~~ its CPS~~s~~:

- What name forms shall be used,
- How the FBCA, Agency CAs and RAs will interact with the Federal PKI Policy Authority to ensure this is accomplished, and
- How they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith"

leaves a CA's community of Subscribers, and a new, different "Joe Smith" enters the community of Subscribers, how will these two people be provided unique names?).

Practice Note: The FBCA considers it good practice for agencies to include the preceding information in the agency's CPS.

Item 3, Section 3.1.7

3.1.7 Method to prove possession of private key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the FBCA or Agency CA. The FBCA or Agency CA shall then validate the signature using the party's public key. The Federal PKI Policy Authority may allow other mechanisms that are at least as secure as those cited here.

In the case where a key is generated directly on the party's hardware or software token, or in a key generator that benignly transfers the key to the party's token, then the party is deemed to be in possession of the private key at the time of generation or transfer. If the party is not in possession of the token when the key is generated, then the token (e.g., a smartcard or a PKCS #12 encoded message) shall be delivered to the subject via an accountable method (see Section 6.1.2).

For all assurance levels, when keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The FBCA (or Agency) must maintain a record of validation for receipt of the token by the subject. When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the FBCA (or Agency CA) are the only recipients of this shared secret.

Item 4, Section 3.1.10,

3.1.10 Authentication of component identities

Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the component must have a human sponsor. The PKI sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)

- Contact information to enable the CA or RA to communicate with the sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).

In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.1.9.

Item 5, Section 4.1.1

4.1.1 Delivery of public key for certificate issuance

Public keys must be delivered for certificate issuance in a way that binds the applicant Agency's verified identification to the public key. For all levels of assurance, this binding may be accomplished using cryptography. If cryptography is used, it must be at least as strong as that employed in certificate issuance. Additionally, for Medium and Basic Assurance, this binding may also be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a hardware or software token to a certificate issuer for local key generation at the point of certificate issuance or request. For Rudimentary Assurance, no trusted delivery mechanism is required. For Test Assurance, the mechanism shall be set forth in the MOA. In all cases, the method used for public key delivery shall be set forth in a CPS.

In those cases where public/private key pairs are generated by the FBCA or Agency CA on behalf of the Subscriber, the FBCA or Agency CA (respectively) shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber. The FBCA or Agency CA (respectively) shall also implement procedures to ensure that the token is not activated by an unauthorized entity.

Item 6, Section 4.2.1

4.2.1 Delivery of Subscriber's private key to Subscriber

In most cases, a private key will be generated and remain within the cryptographic boundary of the cryptographic module. If the owner of the module generates the key, then there is no need to deliver the private key. If the key is generated elsewhere, then the module must be delivered to the Subscriber. Accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. The Subscriber shall acknowledge receipt of the module. Under no circumstances shall

anyone other than the Subscriber have substantive knowledge of or control over private signing keys after generation of the key. Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber. Hardware tokens containing FBCA or Agency CA private signature keys may be backed-up in accordance with security audit requirements defined Section 4.5.1.

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. In these cases:

- An Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.
- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative; and
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

Item 7, Section 4.4.1.2

4.4.1.2 Procedure for revocation request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). Only the Federal PKI Policy Authority or a previously delegated official of the Agency responsible for the Principal CA may direct the Operational Authority to revoke certificates issued by the FBCA. Note that an Agency Principal CA may always revoke the certificate it has issued to the FBCA, thus terminating interoperability with the FBCA without any Federal PKI Policy Authority action.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's or the RA's revocation request must so indicate. If a RA performs this on behalf of a Subscriber, a formal, signed message format known to the CA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.

Upon receipt of a revocation request involving an FBCA certificate, the FBCA Operational Authority shall authenticate the request and apprise the Federal PKI Policy Authority. The Federal PKI Policy Authority may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the Federal PKI Policy Authority shall direct the FBCA Operational Authority to revoke the certificate by placing its serial number and other identifying

information on a CARL/CRL and then post the CARL/CRL in the FBCA repository, in addition to any other revocation mechanisms used. Practice Note: Agency CAs may use OCSP to distribute status information instead of CARL/CRL.

For PKI implementations using hardware tokens, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber's certificates associated with the unretrieved tokens shall be immediately revoked. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

Item 8, Section 4.4.1.4

4.4.1.4 Revocation of a Certificate Issued by an Agency CA

Revocation shall take effect upon the publication of status information (identifying the reason for the revocation, which may include loss, compromise, or termination of employment) within the time limits as specified in Section 4.4.3 (starting from the time the request is authenticated or sufficient evidence of compromise or loss is received). Information about a revoked certificate shall remain in the status information until the certificate expires ~~and for one additional CRL beyond that point~~. A certificate may be removed from the second CRL issued after it expires.

Item 9, Section 4.5.2

4.5.2 Frequency of processing data

Audit logs shall be reviewed in accordance to the table below. The FBCA OA shall explain a~~A~~ll significant events ~~shall be explained~~ in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

{table omitted}

Item 10, Section 4.5.4

4.5.4 Protection of security audit data

The audit process shall not be done by or under the control of the FBCA Operational Authority (or comparable authority for an Agency CA). Agency CA and FBCA system configuration and procedures must be implemented together to ensure that:

- only authorized people have read access to the logs;
- only authorized people may archive ~~or delete~~ audit logs; and ,
- audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from ~~deletion or~~ destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the FBCA equipment. Practice Note: If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived.

Item 11, Section 4.6.2

4.6.2 Retention Period for Archive

{preceeding table and paragraph omitted}
If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternately, an agency may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall also be maintained for a period determined by the Federal PKI Policy Authority for the FBCA (or Agency for the Agency CA).

Item 12 Section 4.8.3 FBCA or Agency CA signature keys are compromised

If the FBCA or Agency CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The Federal PKI Policy Authority and all of its member agencies shall be securely notified at the earliest feasible time (so that agencies may issue CARLs revoking any cross-certificates issued to the FBCA);
- ~~The CAs that have issued certificates to the affected CA shall publish a CARL revoking the affected CA's certificate as set forth above;~~
- A new FBCA or Agency CA key pair shall be generated by the FBCA or Agency CA in accordance with procedures set forth in the FBCA or Agency CPS; and
- New FBCA or Agency CA certificates shall be issued to Agencies also in accordance with the FBCA or Agency CPS.

The FBCA Operational Authority or Agency CA governing body shall also investigate and report to the Federal PKI Policy Authority what caused the compromise or loss, and what measures have been taken to preclude recurrence.

Item 13 Section 5.2.3 Number of persons required per task

To best ensure the integrity of the FBCA equipment and operation, no individual will be assigned more than one trusted role. The separation provides a set of checks and balances over the FBCA operation.

Under no circumstances shall the incumbent of another FBCA role perform its own auditor function.

The requirements of this section apply to agency CAs operating at the high level.

Item 14 Section 6.2.4.1 Backup of FBCA and Agency CA private signature key

If backed up, t~~T~~he FBCA and Agency CA private signature keys shall be backed up under the same multi-person control as the original signature key. ~~Such backup shall create only a~~A single copy of the signature key may be stored at the FBCA or CA location respectively.; ~~a~~ A ~~second~~ copy may be kept at the FBCA or CA backup location~~, respectively~~. Procedures to effect this shall be included in the FBCA CPS.

Item 15, Glossary

Insert the definition for token: Hardware or software that contains or can be used to generate cryptographic keys. Examples of hardware tokens include smart cards and memory cards. Software tokens include messages that contain keys (e.g., PKCS #12 messages) and software that stores or generates keys.

Estimated Cost:

There is no financial cost associated with implementing this change.

Implementation Date:

This change will be implemented immediately.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: 9 May 2002 and 10 May 2002
Date CPWG recommended approval: 9 May 2002 and 10 May 2002
Date Presented to FPKI PA: 18 June 2002
Date of approval by FPKI PA: 18 June 2002